IN THE CLAIMS:

Claims 1-6, 9-15, 18-23, and 26-33 are amended. No claims are cancelled or added. All pending claims and their present status are produced below.

1. (Currently amended) A method for providing [[a]] unique ~~identification~~ identifications of monitored network data instances flowing across various connections between networked devices, the unique ~~identification~~ identifications being derived from information contained entirely within each instance of ~~the~~ network data, the method comprising:

using ~~at least one~~ a monitoring device to monitor a network data instance flowing across ~~at least one~~ a data connection;

deriving from the data instance certain information which collectively provides a unique identification of the network data instance;

assembling the derived information into an input string for a hash function; and

using ~~the~~ an output string of the hash function as a signature which represents a unique identifier of the network data instance.

2. (Currently amended) The method according to Claim 1, wherein the deriving step includes:

deriving from the data instance a source and destination address for the data instance;

deriving from the data instance a source and destination port associated with the networked devices; and

deriving from the data instance ~~at least one~~ a sequence number associated with data instance.

3. (Currently amended) The method according to Claim 1, which further includes:

attaching the signature to ~~at least one~~ a data report associated with the network data instance; and

transmitting the data ~~reports~~ report and the ~~signatures~~ signature from ~~each~~ the monitoring device to a central collecting device.

4. (Currently amended) The method according to Claim 3, wherein a timestamp is further associated with ~~each~~ the data report before it is transmitted to the central ~~collector~~ collecting device.

5. (Currently amended) The method according to Claim 3, wherein the central collecting device uses the ~~signatures~~ signature to eliminate duplicate data reports that might come in from different monitoring devices positioned at different locations on ~~the~~ a network.

6. (Currently amended) The method according to Claim [[1]] 2, wherein the network data instances ~~are~~ include data packets as part of a TCP/IP (Transmission Control Protocol/Internet Protocol) client-server network.

7. (Original) The method according to Claim 6, wherein the source and destination addresses include a client IP address and a server IP address.

8. (Original) The method according to Claim 7, wherein the source and destination port include a client port number and a server port number.

9. (Currently amended) The method according to Claim 2, wherein the ~~at least one~~ sequence number includes a client sequence number or a server sequence number.

10. (Currently amended) The method according to Claim 9, wherein the ~~at least one~~ sequence number includes both a client sequence number and a server sequence number.

11. (Currently amended) The method according to Claim [[2]] 1, wherein the input string ~~information~~ does not include a sequence ~~numbers~~ number.

12. (Currently amended) The method according to Claim [[11]] 1, wherein the network data instances ~~are~~ include datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol) network.

13. (Currently amended) The method according to Claim 1, which further includes [[:]] truncating the signature to include fewer bits than the hash function output string.

14. (Currently amended) The method according to Claim 1, which further includes [[:]] adding flag bits to the signature which indicate ~~the~~ a type of application associated with the network data instance.

15. (Currently amended) The method according to Claim 3, wherein the ~~monitor~~ monitoring device serves as a data reduction device for data report and signature information being sent to the central ~~data collector~~ collecting device.

16. (Original) The method according to Claim 1, wherein the monitoring device operates to directly monitor the network data.

17. (Original) The method according to Claim 1, wherein the monitoring device operates to indirectly monitor the network data.

18. (Currently amended) An apparatus for providing [[a]] unique ~~identification~~ identifications of monitored network data instances flowing across various connections between networked devices, the unique ~~identification~~ identifications

being derived from information contained entirely within each instance of ~~the~~ network data, the apparatus comprising:

~~at least one~~ a monitoring device positioned to monitor a network data instance flowing across ~~at least one~~ a data connection;

a hash function device having an input string and an output string, the input string assembled from certain information derived from the network data instance, the information collectively providing a unique identification of the network data instance;

wherein the output string is used as a signature which represents a unique identifier of the network data instance.

19. (Currently amended) The apparatus according to Claim 18, wherein the information derived from the network data instance includes at least:

a source and destination address derived from the network data instance;

a source and destination port associated with the networked devices; and

~~at least one~~ a sequence number associated with network data instance.

20. (Currently amended) The apparatus according to Claim 18, which further includes:

~~at least one~~ a data report associated with the network data instance, the signature being attached to the data report; and

a central collection device that receives ~~transmitted~~ the data ~~reports~~ report and ~~signatures~~ the signature from ~~each~~ the monitoring device.

21. (Currently amended) The apparatus according to Claim 20, wherein a timestamp is further associated with ~~each~~ the data report before it is transmitted to the central ~~collector~~ collection device.

22. (Currently amended) The apparatus according to Claim 20, wherein the central ~~collecting~~ collection device uses the ~~signatures~~ signature to eliminate duplicate data reports that might come in from different monitoring devices positioned at different locations on ~~the~~ a network.

23. (Currently amended) The apparatus according to Claim 19, wherein the network data instances ~~are~~ include data packets as part of a TCP/IP (Transmission Control Protocol/Internet Protocol) client-server network.

24. (Original) The apparatus according to Claim 23, wherein the source and destination addresses include a client IP address and a server IP address.

25. (Original) The apparatus according to Claim 24, wherein the source and destination port include a client port number and a server port number.

26. (Currently amended) The apparatus according to Claim 25, wherein the ~~at least one~~ sequence number includes a client sequence number or a server sequence number.

27. (Currently amended) The apparatus according to Claim 26, wherein the ~~at least one~~ sequence number also includes both a client sequence number and a server sequence number.

28. (Currently amended) The apparatus according to Claim [[19]] 18, wherein the input string ~~information~~ does not include a sequence ~~numbers~~ number.

29. (Currently amended) The apparatus according to Claim 28, wherein the network data instances ~~are~~ include datagrams as part of a UDP/IP (User Datagram Protocol/Internet Protocol) network.

30. (Currently amended) The ~~method~~ apparatus according to Claim 18, wherein the signature is truncated to include fewer bits than the hash function output string.

31. (Currently amended) The ~~method~~ apparatus according to Claim 18, wherein flag bits are added to the signature which indicate ~~the~~ a type of application associated with the network data instance.

32. (Currently amended) The ~~method~~ apparatus according to Claim 20, wherein the ~~monitor~~ monitoring device serves as a data reduction device for the data report and the signature ~~information~~ being sent to the central ~~data collector~~ collection device.

33. (Currently amended) A method for providing [[a]] unique ~~signature~~ signatures of monitored network data packets flowing across various connections between networked devices, the unique ~~signature~~ signatures being derived from information contained entirely within each instance of the network data ~~packet~~ packets, the method comprising:

using ~~at least one~~ a monitoring device to monitor a network data packet flowing across ~~at least one~~ a data connection;

deriving from the data packet a source and destination address for the data packet;

deriving from the data packet a source and destination port associated with the networked devices;

deriving from the data packet ~~at least one~~ a sequence number associated with the data ~~instance~~ packet;

assembling the derived addresses, ports, and ~~at least one~~ the sequence number ~~information~~ into an input string for a hash function;

using ~~the~~ an output string of the hash function as ~~the~~ a signature which represents a unique identifier of the network data packet;

attaching the signature to ~~at least one~~ a data report associated with the network data packet; and

transmitting the data ~~reports~~ report and ~~signatures~~ signature from ~~each~~ the monitoring device to a central collecting device for analysis.